DNSSEC Operational Practices, Version 2

Editors:
Olaf Kolkman & Miek Gieben

Administration

- draft-ietf-dnsop-rfc4641bis-01
- http://www.nlnetlabs.nl/svn/rfc4641bis/trunk/open-issues/
- Version 00 of the document:
  - Is RFC4641 with errata corrected;
  - With trivial IANA considerations added;
  - And with references reordered (XML playing tricks)

Should we target for BCP?

- 4641 is informational: DNSSEC is all so new, it is difficult to make the case that there is a set of practices that is well tested and therefore "best"
- Should we target for BCP this time?

Key Size considerations

- Removed the table of key sizes and simplified the recommendation: 1024bit keys will do in most cases, 2048 is the next alternative.
- These considerations will need review by crypto specialists.

Differentiation between KSKs used in different context (DS vs Trust Anchor)

- Added some differentiation between keys that act as KSK when KSKs are used as trust-anchors by third parties, other stability considerations apply then when KSKs are just used.

Key Effectivity Periods

- KSK key effectivity period 2 decades or;
- KSK key effectivity 12 months?
- Key question: Is rolling the key (that may be configured as a trust anchor) worth the stability risk?
  - Roll often and experience and awareness is gained and maintained
  - Roll often and you introduce periodic stability risk
- Guidance needed

Key Algorithm Rollover

- Added Key Algorithm Rollover description (section 4.2.4)
- In essence a double signature rollover.
- taking into account the downgrade 'requirements': there must be a signature for each algorithm for which there is a key.

(Non-)cooperative registrars

- Added a section about how to proceed when a zone is moved from one operator to the other.
- Assuming the operators are cooperative, but do not pass private key material around
- Also added some words on non-cooperative registrars
  - The picture looks dim, specifically in the case when extremely long TTLs are used by the 'originating' registry.
  - Also an issue without DNSSEC